Политика AML/Политика «Знай своего клиента»

ВВЕДЕНИЕ

Компания BIT TRADE MARKETS OÜ, зарегистрированная в Эстонии (регистрационный номер 14555301) (далее «Компания»), представляет положения Политики AML и Политики «Знай своего клиента» (далее «Политика AML и Политика «Знай своего клиента»), которые предназначены для предотвращения и уменьшения возможных рисков Компании, связанных с вовлечением ее в любую незаконную деятельность.

Как международные, так и местные положения требуют от Компании внедрения эффективных внутренних процедур и механизмов предотвращения отмывания денег, финансирования терроризма, торговли наркотиками и людьми, предотвращения распространения оружия массового уничтожения, коррупции и взяточничества и принятия мер в случае какой-либо подозрительной деятельности Клиентов Компании.

Политика AML и Политика «Знай своего клиента» регулирует:

- Процедуры верификации;
- Сотрудника отдела комплаенс;
- Мониторинг транзакций;
- Оценку рисков.

1. ПРОЦЕДУРЫ ВЕРИФИКАЦИИ

Надлежащая проверка клиентов (CDD — Customer Due Diligence) является одним из международных стандартов предотвращения незаконной деятельности. Согласно CDD, Компания устанавливает свои собственные процедуры верификации в рамках положений и стандартов по борьбе с отмыванием денег и политики «Знай своего клиента».

1.1. ПРОВЕРКА ЛИЧНОСТИ

Для прохождения процедуры проверки личности Пользователю необходимо представить Компании надежные документы от независимых источников, данные или информацию (например, национальное удостоверение личности, международный паспорт, выписку из банка, счет за коммунальные услуги). С целью соблюдения Политики AML и Политики «Знай своего Клиента» Компания оставляет за собой право запрашивать идентификационные данные Пользователя.

Компания предпримет шаги для подтверждения подлинности документов и информации, предоставляемой Пользователями. Будут применены все юридические меры для перепроверки идентификационных данных. Компания оставляет за собой право собирать сведения по Пользователям, которые были отнесены к категории опасные или подозрительные.

Компания оставляет за собой право осуществлять проверку личности Пользователя на постоянной основе, особенно если Пользователь изменил идентификационные данные, или если его деятельность показалась подозрительной (необычной для конкретного Пользователя). Кроме того, Компания оставляет за собой право запрашивать у Пользователей обновленные документы, даже если ранее они прошли верификацию.

Сбор, хранение, разглашение и защита идентификационных данных Пользователя будет

осуществляться строго в соответствии с Политикой конфиденциальности и правилами Компании.

Как только личность Пользователя установлена, Компания может отказаться от потенциальной юридической ответственности в ситуации, если Услуги Компании используются Пользователем для осуществления незаконной деятельности.

1.2. ПРОВЕРКА КАРТЫ

Пользователи, которые намерены использовать платежные карты для работы с Продуктами и Услугами Компании, должны пройти проверку карты согласно инструкциям на сайте Компании.

2. СОТРУДНИК ОТДЕЛА КОМПЛАЕНС

Сотрудник отдела комплаенс является лицом, которое должным образом уполномочено Компанией, чья обязанность заключается в эффективном осуществлении и обеспечении соблюдения Политики AML и Политики «Знай своего Клиента». Обязанностью сотрудника отдела комплаенс является контроль всех аспектов политики Компании по противодействию отмыванию денег и финансированию терроризма, в том числе, включая:

- **a.** Сбор идентификационных данных Пользователей;
- **b.** Создание и обновление внутренних политик и процедур для завершения, рассмотрения, представления и хранения всех отчетов и записей, требуемых в соответствии с действующими законами и правилами;
- **c.** Мониторинг транзакций и исследование любых существенных отклонений от стандартной деятельности;
- **d.** Внедрение системы управления записями для соответствующего хранения и поиска документов, файлов, форм и журналов;
- **e.** Регулярное обновление оценки риска;
- **f.** Предоставление правоохранительным органам необходимой информации в соответствии с действующими законами и правилами.

Сотрудник отдела комплаенс имеет право взаимодействовать с правоохранительными органами, которые занимаются предотвращением отмывания денег, финансирования терроризма и другой незаконной деятельности.

3. МОНИТОРИНГ ТРАНЗАКЦИЙ

Личность Пользователей устанавливается не только путем проведения их идентификации (кем они являются), но, что еще более важно, путем анализа шаблонности их транзакций (что они делают). Таким образом, Компания использует анализ данных как инструмент оценки риска и выявления подозрительной активности. Компания выполняет множество задач по соответствию существующим требованиям, в том числе сбор и сортировка данных, ведение записей, управление процессами сбора сведений и предоставление отчетности. Функциональные возможности системы включают в себя следующее:

1) Ежедневная проверка Пользователей по общепризнанным «черным спискам» (например, OFAC), объединение переводов по нескольким точкам данных, внесение Пользователей в список наблюдения и отказа в предоставлении услуг, открытие дел для проведения расследования (при необходимости), отправка внутренней коммуникации и заполнение обязательных отчетов (при необходимости);
2) Управление документацией;
3) Отслеживание шаблонов поведения Клиентов.

В соответствии с Политикой AML и Политикой «Знай своего Клиента», Компания обязуется отслеживать все транзакции и оставляет за собой право:

- гарантировать, что сотрудник отдела комплаенс будет сообщать надлежащим правоохранительным органам о транзакциях подозрительного характера;
- запрашивать у Пользователя какую-либо дополнительную информацию или документы в случае возникновения подозрительных транзакций;
- приостанавливать или прекращать действие (использование) Личного Кабинета Пользователем, когда у Компании есть достаточные основания подозревать Пользователя в незаконной деятельности;
- представленный выше перечень является неполным, и отслеживание транзакций Пользователей будет осуществляться сотрудником отдела комплаенс на регулярной основе для того, чтобы определить, относятся ли транзакции к подозрительным, и стоит о них сообщать или нет.

4. ОЦЕНКА РИСКОВ

Компания в соответствии с международными требованиями использовала подход, основанный на оценке риска, для борьбы с отмыванием денег и финансированием терроризма. Используя подход, основанный на оценке риска, Компания может обеспечить, чтобы меры по предотвращению или уменьшению отмывания денег и финансирования терроризма были соизмеримы с выявленными рисками. Это позволит распределить ресурсы наиболее эффективным образом. Принцип заключается в том, что ресурсы должны быть направлены в соответствии с приоритетами таким образом, чтобы наибольшим рискам уделялось наибольшее внимание.